Deloitte
Statsautoriseret
Revisionspartnerselskab
CVR-nr. 33 96 35 56
Weidekampsgade 6
2300 København S

Telefon: 36102030
www.deloitte.dk

ISAE 3402 type 2-erklæring

Uafhængig revisors erklæring om VUCHostings kontroller, deres udformning, implementering og funktionalitet i tilknytning til VUCHostings hostingydelse for perioden fra 01.01.2021 til 31.12.2021

Indholdsfortegnelse

1 Serviceleverandørs uafhængige revisors erklæring med sikkerhed

Serviceleverandørs uafhængige revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet

Til: ledelsen hos VUCHosting

Omfang

Vi har fået til opgave at afgive erklæring om VUCHostings beskrivelse i afsnit 3, VUCHostings systembeskrivelse af VUCHostings hostingydelse til behandling af kunders transaktioner i hele perioden fra 1. januar 2021 til 31. december 2021 (beskrivelsen) og om udformningen og funktionaliteten af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

VUCHosting har anvendt serviceunderleverandøren EG A/S til udvikling og vedligeholdelse af Ludus Suite samt GlobalConnect A/S til fysisk housing af servere. Endvidere anvender VUCHosting serviceunderleverandøren Atea Managed Service til ekstern backup. Serviceleverandørens systembeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos serviceunderleverandørerne. Denne erklæring er udarbejdet efter partielmetoden og omfatter således ikke kontroller hos serviceunderleverandørerne.

Nogle af de kontrolmål, der er anført i VUCHostings beskrivelse af hostingydelsen kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos VUCHosting. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementerende kontroller.

VUCHostings ansvar

VUCHosting er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i afsnit 2, "VUCHostings udtalelse", herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret, for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for udformningen, implementeringen og funktionaliteten af kontroller for at nå de anførte kontrolmål.

Vores uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i IESBA's Etiske regler, som er baseret på grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd.

Deloitte anvender ISQC 1 og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder samt gældende krav ifølge lov og øvrig regulering.

Serviceleverandørens revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om VUCHostings beskrivelse samt om udformningen og funktionaliteten af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3402, *Erklæringer med sikkerhed om kontroller hos en serviceleverandør*, som er udstedt af IAASB. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system samt for kontrollernes udformning og funkti-

onalitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev nået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte kontrolmål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet i afsnit 2, "VUCHostings udtalelse".

Det er vores opfattelse, at det opnåede bevis er tilstrækkeligt og egnet til at danne grundlag for vores konklusion.

Begrænsninger i kontroller hos en serviceleverandør

VUCHostings beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved systemet, som hver enkelt kunde måtte anse for vigtige efter deres særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller opdage alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en serviceleverandør kan blive utilstrækkelige eller svigte.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i afsnit 2. Det er vores opfattelse,

(a) at beskrivelsen af kontroller, således som det var udformet og implementeret i hele perioden fra 1. januar 2021 til 31. december 2021, i alle væsentlige henseender er retvisende
(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 1. januar 2021 til 31. december 2021, og
(c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev nået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. januar 2021 til 31. december 2021.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater af disse test fremgår af afsnit 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt kunder, der har anvendt VUCHostings hostingydelse, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kunders egne kontroller, når de vurderer risiciene for væsentlig fejlinformation i deres regnskaber.

København, den 18. januar 2022

Deloitte
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 96 35 56

Thomas Kühn
statsautoriseret revisor

2 Serviceleverandørs udtalelse

VUCHostings udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt VUCHostings hostingydelse, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som kunderne selv har anvendt, ved vurdering af risiciene for væsentlig fejlinformation i kundernes regnskaber. VUCHosting bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en retvisende beskrivelse af VUCHostings hostingydelse, der har behandlet kunders transaktioner i hele perioden fra 1. januar 2021 til 31. december 2021. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

i. redegør for, hvordan systemet var udformet og implementeret, herunder redegør for:
   - de typer af ydelser, der er leveret, herunder behandlede grupper af transaktioner, når det er relevant
   - de processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere transaktionerne samt overføre disse til de rapporter, der er udarbejdet til kunder
   - de tilhørende regnskabsregistreringer, underliggende information og specifikke konti, der blev anvendt til at igangsætte, registrere, behandle og rapportere transaktioner, herunder korrektionen af ukorrekt information, og hvordan information blev overført til de rapporter, der er udarbejdet til kunder
   - hvordan systemet behandlede andre betydelige begivenheder og forhold end transaktioner
   - den proces, der blev anvendt til at udarbejde rapporter til kunder
   - relevante kontrolmål og kontroller udformet til at nå disse mål
   - kontroller, som vi med henvisning til systemets udformning har forudsat ville være implementeret af brugervirksomheder, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen sammen med de specifikke kontrolmål, som vi ikke selv kan nå
   - andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen og rapporteringen af kunders transaktioner.

ii. indeholder relevante oplysninger om ændringer i serviceleverandørens system foretaget i perioden fra 1. januar 2021 til 31. december 2021.

iii. ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne system, under hensyntagen til at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved systemet, som den enkelte kunde måtte anse for vigtigt efter deres særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 1. januar 2021 til 31. december 2021. Kriterierne for denne udtalelse var, at:

i. de risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret
ii. de identificerede kontroller ville, hvis anvendt som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål, og
iii. kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. januar 2021 til 31. december 2021.

København, den 18. januar 2022

VUCHosting

Anita Lindquist
rektor

3 Serviceleverandørens systembeskrivelse

Virksomheden og vores ydelse

KVUC er værtsinstitution for et administrativt samarbejde om det studieadministrative system Ludus Suite. I den forbindelse er det blevet aftalt at KVUC hoster og drifter Ludus Suite for alle landets VUC'er. KVUC har derfor stiftet VUCHosting, som har fysisk adresse sammen med KVUC. VUCHosting blev etableret september 2013.

Til varetagelse af hosting-opgaven er der etableret en organisation bestående af en økonomichef, en projektleder, en driftsansvarlig – herunder 3 yderligere medarbejdere i driftsafdelingen og 2 hotline-medarbejdere.

VUCHostings målsætning er først og fremmest, at driften af Ludus Suite hostes sikkert og stabilt og efter aftalte Service Level Agreements. Sekundært er det VUCHostings målsætning af supportere og opkvalificere Ludus-superbrugere på det enkelte VUC i Ludus Suite og omkringliggende it-miljø.

VUCHosting deltager via projektleder aktivt i udvikling af Ludus Suite, og derfor er vi altid på forkant med kommende udvikling på softwaren og kan tilpasse eventuelle nye driftsbehov.

Generelt om vores kontrolmål og implementerede kontroller

Vores generelle beskrivelse af kontrolmål og implementerede kontroller:

Vi har defineret vores kvalitetsstyringssystem ud fra vores overordnede målsætning om at levere stabil og sikker it-drift til vores kunder. For at kunne gøre det har vi politikker og om nødvendigt procedurer, der sikrer et højt niveau af dokumenteret it-sikkerhed.

Vores it-sikkerhedspolitik er udarbejdet med reference til ovenstående og er gældende for alle medarbejdere og for alle leverancer.

Vores metodik for implementering af kontroller er defineret med reference til ISO 27002 og er dermed helt overordnet inddelt i de herpå følgende kontrolområder:

- 4 - Risikovurdering og -håndtering
- 5 - Sikkerhedspolitik
- 6 - Organisering af informationssikkerhed
- 7 - Sikkerhed i forhold til HR
- 8 - Styring af aktiver
- 9 - Adgangskontrol
- 10 - Kryptografi
- 11 - Fysisk og miljømæssig sikring
- 12 - Sikkerhed i forbindelse med drift
- 13 - Kommunikationssikkerhed
- 14 - Anskaffelse, udvikling og vedligeholdelse
- 15 - Leverandørforhold
- 16 - Styring af sikkerhedshændelser
- 17 - Informationssikkerhedsaspekter ved beredskabsstyring
- 18 - Overensstemmelse.

Det følgende beskriver vores kontrolmiljø nærmere for hvert enkelt område.

Organisation og ansvar

VUCHosting beskæftiger 8 medarbejdere, og er inddelt i ansvarsområderne ledelse, kursus, udvikling, hotline og drift. Hotline varetager first level support af Ludus Suite og omkringliggende it-miljø, og kan eskalere sager til second level support hos drift, projektleder eller systemleverandør.

It-chefen på KVUC har det daglige ansvar for den samlede mængde af opgaver vedrørende hosting af Ludus Suite samt personaleledelse på driftsområdet. Projektlederen har ansvaret for den daglige ledelse af VUCHostings aktiviteter på udvikling, kursus, support og økonomi. Økonomichefen på KVUC har ansvaret for formel budgetopfølgning og regnskabsaflæggelse samt personaleledelse for hotline og projektleder. Den øverste leder på KVUC har det endelige ansvar for it-sikkerheden i VUCHosting, leverandør, udløb af serviceaftaler mv.

4 Rikovurdering og håndtering

4.1 Risikovurdering

4.1.1 It-risikoanalyse og -vurdering

Der er senest i november 2021 udført en risikoanalyse – denne er ledelsesgodkendt af KVUC's øverste leder og giver ikke anledning til igangsættelse af handlingsplan.

Næste vurdering foretages senest november 2022, medmindre ændringer i VUCHostings organisation eller it-miljø giver anledning til at foretage en ny vurdering ad hoc. Ændringer, der kan give anledning til en ad hoc analyse, inkluderer leverandørskift, personaleudskiftning, manglende it-revision hos leverandør, udløb af serviceaftaler mv.

4.2 Håndtering af sikkerhedsrisici

4.2.1 Procedure for risikohåndtering

Risikoanalysen udgøres af vurdering af vitale afhængigheder som hver gennemgås i forhold til sandsynlighed, påvirkning og mulig imødegåelse. Hver afhængighed leverer en risikofaktor, som opsummeres pr. hovedservice (Ludus og Ludus Web).

Det er ledelsens beslutning at risikovurderingen ikke må overstige en samlet faktor for hver subservice på 25. For hovedservicen Ludus kan en subservice eksempelvis være datacentrets fysiske faciliteter. Her vurderes det, hvilken impact de fysiske faciliteter kan have på leveringen af Ludus. Har datacentret eksempelvis den fornødne brandhæmning, nødstrøm osv. Ud fra status af de fysiske faciliteter vurderes en sandsynlighed for påvirkning på levering af Ludus, som sammen med den vurderede impact udgør en faktor. Ludus har samlet set 7 forskellige subservices, som leveringen af den er afhængig af – hver af de 7 subservices faktorer udgør en samlet faktor, som ikke må overstige 25, uden at dette skal godkendes som en særlig risiko og udløse en ny version af risikoanalysen, hvor subservicen og dens afhængigheder gennemgås, og handlingsplan for imødegåelse af afhængighedernes risiko igangsættes, således at den samlede faktor hurtigst muligt kan nedbringes til 25 eller lavere.

For at sikre at risikovurderingen bliver udført ofte nok, dagsordensættes det halvårligt på driftsmøde i den daglige ledelse.

5 Sikkerhedspolitik

5.1 It-sikkerhedspolitik

5.1.1 It-sikkerhedspolitik

Der er til enhver tid en gældende sikkerhedspolitik for VUCHosting, som indeholder nøglepunkter fra ISO 27002 og har til mål at beskrive gennemskuelige politikker med fokus på driftssikkerhed og gennemskuelighed for det administrative fællesskabs deltagende VUC'er.

5.1.2 Evaluering af it-sikkerhedspolitikken

Sikkerhedspolitikken revideres minimum årligt. For at sikre at risikovurderingen bliver udført ofte nok, dagsordensættes det halvårligt på driftsmøde i den daglige ledelse.

6 Organisering af informationssikkerhed

6.1 Intern organisering

6.1.1 Delegering af ansvar for informationssikkerhed

Vi har en klar opdelt organisation, hvad ansvar angår, og har udførlige ansvars- og rollebeskrivelser på alle arbejdsområder i VUCHosting. Herunder både drift, support, kursus og ledelse.

6.1.2 Funktionsadskillelse

Funktionsadskillelse er en vigtig del af vores organisation og drift, hvorfor vi, via adgangskontroller og rettighedsstyring, sikrer, at kun autoriseret personale kan udføre de nødvendige handlinger på systemerne. Det er derfor kun driften, der kan udføre driftsrelaterede procedurer osv.

6.1.5 Informationssikkerhed som en del af projektstyring

Vi tager altid stilling til it-sikkerhed i vores projekter uanset type og størrelse og følger en fast procedure for datasikkerhed i processen samt generel it-sikkerhed i valg af leverandør.

6.2 Mobilt udstyr og fjernarbejdspladser

6.2.1 Politik for mobile enheder

Adgang til Ludus web kan og må ske fra mobile enheder, da det er en webapplikation. Adgang til Ludus via Citrix kan ikke og må ikke ske fra mobile enheder. Dette er et designvalg, da Ludus ikke understøtter mobiladgang.

6.2.2 Fjernarbejdspladser

Adgang til systemerne skal ske via sikre og brugervenlige kanaler. Driftsansatte i VUCHosting kan kun tilgå VUCHostings systemer via VPN. Dette kan gøres fra medarbejderens udleverede PC eller fra privat udstyr. Hotline og ledelse har kun adgang via Citrix og med NemID-godkendelse.

7 Sikkerhed i forhold til ansættelse

7.1 Inden ansættelse

7.1.1 Screening

Ansættelse af nye medarbejdere skal som hovedregel ske via forskellige eksterne samarbejdspartnere; eksempelvis rekrutteringsbureauer. Der kan dog også i særlige tilfælde anvendes intern rekruttering eller direkte opslag. Hvis der anvendes direkte opslag, er det ledelsens ansvar at screene kandidater. Det er ledelsen opgave at sørge for, at rekrutteringsbureauet finder relevante kandidater. Ved ansættelsessamtaler skal der være en repræsentant fra ledelse samt for medarbejdergruppen.

7.1.2 Ansættelsesforhold

Generelle vilkår for ansættelse følger gældende overenskomster. I tillægget til den ansattes kontrakt med KVUC anføres eventuelle særlige forhold vedrørende fortrolighed i forbindelse med adgang til personfølsomme oplysninger for VUCHostings kunder samt evt. strafansvar i forbindelse med denne tavshedspligt.

7.2 Under ansættelse

7.2.1 Ledelsens ansvar

Ledelsen har ansvaret for, at der implementeres og vedligeholdes et tilstrækkeligt informationssikkerhedsniveau hos medarbejderne i VUCHosting.

7.2.2 Bevidsthed om uddannelse og træning i informationssikkerhed

Vores aktiver er i høj grad vores medarbejdere, og der er derfor løbende fokus på udvikling af vores medarbejderes kvalifikationer og uddannelse.

Der anvendes eksterne kurser og konferencer for at sikre, at medarbejdere opnår nye kompetencer, der kan matche virksomhedens behov. Der gennemføres medarbejderudviklingssamtaler årligt, og disse skal udmunde i en skriftlig aftale imellem ansat og leder.

Hvis ny lovgivning inden for informations- eller datasikkerhed træder i kraft, er det ledelsens ansvar at informere de ansatte og sikre, at deres kompetenceniveau svarer til kravene i en ny lovgivning. Plan for dette drøftes og vedtages på driftsmøde i den daglige ledelse.

7.3 Ansættelsesforholdets ophør eller ændring

7.3.1 Ophør eller ændring i ansættelse

Generelle vilkår for ophør i ansættelse er angivet i hver medarbejders ansættelseskontrakt. Ansvaret for at rettigheder og adgange annulleres ved ansættelsesophør ligger hos den driftsansvarlige, som skal informeres om ansættelsens ophør af vedkommendes personaleleder.

8 Styring af aktiver

8.1 Ansvar for aktiver

8.1.1 Fortegnelse over aktiver

Hardware i anvendelse i driften (servere m.m.) er dokumenteret i oversigter. Udleveret udstyr (mobil, pc) er dokumenteret med udleveringsblanketter, som kan bruges ved tilbagelevering. Dokumentation over hardware i anvendelse i driften (servere m.m.) opdateres af den driftsansvarlige ved ændringer. Tjek af om oversigten over hardware er opdateret, udføres halvårligt ved at punktet tages op på driftsmøde i den daglige ledelse.

8.1.2 Ejerskab af aktiver

Centrale netværksenheder, servere, periferienheder og lign. er tilegnet den driftsansvarlige, som er system- og aktivejer.

8.1.3 Klassifikation af information

Jævnfør VUCHostings sikkerhedspolitik kan data klassificeres som kundeejet, ekstern eller ekstern fortrolig.

8.1.4 Tilbagelevering af aktiver

Tilbagelevering af udleverede pc'er og mobile enheder sker straks efter endt ansættelse. Udstyr kan ikke købes fri, og der skal kvitteres for aflevering.

8.3 Mediehåndtering

8.3.2 Bortskaffelse af medier

Bortskaffelse af medier, som er defekte, eller ikke skal være i brug længere, sker via aftaler med leverandør.

9 Adgangskontrol

9.1 Forretningskrav til adgangskontrol

9.1.1 Politikker for adgangsstyring

Politikker for adgangsstyring er beskrevet i VUCHostings gældende sikkerhedspolitik.

9.2 Administration af brugeradgang

9.2.1 Brugeroprettelses- og nedlæggelsesprocedure

Brugere vedligeholdes løbende. Hvis en medarbejders ansættelsesforhold stopper i VUCHosting, bliver brugerkontoen deaktiveret i Active Directory og adgangen til incident managementsystem, mailkonto, adgang til drev osv. dermed lukket. Informationen kommer via et medarbejder-flow eller pr. e-mail til it@kvuc.dk. Adm. konti slettes ikke, men deaktiveres blot så historiske data bevares.

Vi kontrollerer jævnligt brugeraktivitet for AD-profiler, og har der ikke været aktivitet i mere end 90 dage, bliver profilen deaktiveret.

9.2.2 Rettighedstildeling

Interne administratorrettigheder i forhold til it-drift godkendes af den it-driftsansvarlige hos VUCHosting. Den driftsansvarlige godkender desuden tildeling af administratorrettigheder til eksterne samarbejdspartnere og hvor længe brugerkonti er aktive. Der tilkendes kun adgang efter udfyldt NDA imellem firma og VUCHosting og udfyldt anmodning om adgang for den enkelte bruger.

Den driftsansvarlige modtager dagligt en e-mail indeholdende hvem der har administratoradgang.

9.2.3 Kontrol med privilegerede adgangsrettigheder

VUC Hosting betegner brugere, som er medlem af Domain Admins, som privilegerede medarbejdere. Privilegerede konti tildeles få personer. Dagligt sendes en aktivitetsrapport til eventlog@kvuc.dk og direkte til den driftsansvarlige, som kontrollerer aktive brugere.

9.2.4 Håndtering af fortrolige logininformationer

Alle ansatte i VUCHosting, som tilgår Citrix via brugerfladen, får via informationsbrev, der medfølger NemID-nøglekort, at vide, at kodeord og nøglekort er personlige og må under ingen omstændigheder deles med andre.

9.2.5 Evaluering af brugeradgangsrettigheder

Alle brugerrettigheder for ansatte i VUCHosting evalueres af den daglige ledelse på driftsmøde årligt.

9.4 Kontrol af adgang til Systemer og data

9.4.1 Begrænset adgang til data

Rettigheder til Citrix styres via sikkerhedsgrupper i Active Directory. Der er oprettet en gruppe for hver skole. Navnestandarden er skolens CVR-nummer.

Adgang til skolens data via Citrix kan åbnes ved at anvende Ludus-applikationen. Det påhviler VUC'et selv at styre brugerrettighederne hertil. Hertil kan skolen tilgå sin data via odbc-forbindelse fra en Excel-installation i Citrix. VUC'et angiver selv til VUCHosting hvilke ansatte, der må få adgang til dette. Yderligere kan skolen tilgå sin data via programmet Crystal Reports.

VUCHosting administrerer kodeord til systemdelen af Ludus Web. Glemte kodeord udleveres efter skriftlig anmodning fra det pågældende VUC til VUCHostings hotline. VUCHosting har på forhånd indsamlet underskrevet tilsagn til hvilke ansatte, der må rekvirere eller nulstille password til systemdelen af Ludus Web.

9.4.2 Procedurer for sikkert log-on

Kundeportal: Anvendelsen af den hostede løsning kan ske igennem en Citrix-løsning, som benytter NemID til brugergodkendelse. Indgangen sker igennem https://portal.vuchosting.dk/, hvor man præsenteres for Nets NemID-applet, der afkræver hhv. brugernavn, password og et engangskodeord fra nøglekort.

Til kursusformål anvendes et sideløbende Citrix-login, som anvendes med prædefinerede kursusbrugere. Disse brugerkonti oprettes og nedlægges alene til kursusformålet og består af et brugernavn og et password. Kursuskonti er kun aktive i den bestilte kursusperiode.

Administration: VUCHostings personale og eksterne samarbejdspartnere har mulighed for at logge på via VPN for at opnå netværksadgang til de bagvedliggende systemer. Adgangen sker via Cisco AnyConnect SSL VPN og benytter credentials fra Active Directory.

9.4.3 System for administration af adgangskoder

Alle interne brugere har en adgangskode, og det er systemmæssigt sat op således, at der er begrænsninger ift. udformningen af kodeordet.

Passwords på domænet er kontrolleret via regler defineret i GPO'er. Systemer, som ikke er en del af domænet, er kontrolleret via specialudviklet værktøj.

Passwords til netværksudstyr skal være komplekse, have en længde på mindst 10 karakterer og indeholde tegn fra mindst 3 tegngrupper. Passwords på netværksudstyr dokumenteres særskilt og skiftes senest hvert halve år. Brugerkonti til netværksenheder opbevares lokalt på enhederne.

10 Kryptografi

10.1 Kontrol med anvendelsen af kryptografi

10.1.1 Politik for anvendelse af kryptografi

VUCHosting anvender kryptografi til VPN-forbindelser mellem VUCHosting og VUC'er eller deres eksterne samarbejdspartnere - eksempelvis driftscentre. Specifikationer for kryptering er beskrevet i den blanket, som VUC eller deres eksterne samarbejdspartner skal udfylde for at få oprettet en VPN-forbindelse.

10.1.2 Administration af krypteringsnøgler

For VPN gælder følgende: Ved udfyldelsen af VPN-blanket aftales en krypteringsnøgle med modparten, hvorefter VUCHosting opdaterer VPN-blanketten. Krypteringsnøglen er gældende i aftalens løbetid.

For SSL gælder følgende: VUCHosting opbevarer både certifikat og den private nøgle. Det er kun den driftsansvarlige og driftsmedarbejderne, der har adgang til dem.

11 Fysisk og miljømæssig sikring

11.1 Sikre områder

11.1.1 Fysisk skalsikring

Leverandør til fysisk placering af servere m.m. er godkendt efter ISAE 3402-standarden.

11.1.2 Fysisk adgangskontrol

Driftsmedarbejderne og den driftsansvarlige har som de eneste adgange til fysisk lokation for servere. Medarbejdere har en udleveret nøglebrik, som de har kvitteret for. VUCHosting har en altid opdateret liste over hvilke medarbejdere, der har fået udleveret en nøglebrik til hosting-centeret.

11.1.3 Sikring af kontorer, lokaler og faciliteter

Driftskontoret hos VUCHosting, som er beliggende hos KVUC, er sikret via ADK, forstærket glas og udvendig videoovervågning. Hændelseslog over adgang til driftskontoret kan udtrækkes til kontrol ved mistanke om misbrug. Adgang til driftskontor er udelukkende tildelt den driftsansvarlige og de driftsansatte samt rengøring og servicepersonel på KVUC.

11.1.4 Beskyttelse mod eksterne og miljømæssige trusler

Vi benytter et hosting-center, som er godkendt efter ISAE 3402-standarden.

11.2 Udstyr

11.2.1 Placering og beskyttelse af udstyr

Vi benytter en leverandør til fysisk opbevaring af servere m.m., som er godkendt efter ISAE 3402-standarden. Bærbare medier og mobile enheder opbevares og anvendes på den enkelte medarbejdes foranledning, dog skal disse aflåses i sikker dock, skuffe eller skab ved endt arbejdsdag, hvis udstyret ikke medtages.

11.2.7 Sikker bortskaffelse eller genbrug af udstyr

Såfremt udstyr skal bortskaffes, træffes aftale med ekstern samarbejdspartner, der har en beskrevet procedure for dette.

11.2.8 Brugerudstyr uden opsyn

VUCHosting stiller krav om, at skærmen skal låses, hvis medarbejderens pc forlades.

11.2.9 Politik for ryddeligt skrivebord og blank skærm

Alle ansatte i VUCHosting er underlagt en clean desk-politik, som inkluderer aflåsning af mobile enheder og bærbart udstyr. Hvis medarbejderen glemmer at låse skærmen, har VUCHosting implementeret system på pc'erne, således at skærmen automatisk låses efter 15 minutter.

12 Sikkerhed i forbindelse med drift

12.1 Operationelle procedurer og ansvarsområder

12.1.1 Dokumenterede driftsprocedurer

VUCHosting har interne driftsprocedurer for vedligeholdelse af systemerne. Driftsprocedurerne opdateres løbende, så de altid er aktuelle.

12.1.2 Ændringsstyring

VUCHostings serviceydelse er Ludus Suite, og der defineres i den sammenhæng forskellige kategorier af ændringer: Periodiske opdateringer, Myndighedskrav, Kritiske opdateringer (incidents af kategori A eller B), Almindeligt vedligehold ved nye versioner af Ludus Suite. Projektlederen skal inden implementering af hver af disse ændringer foretage vurdering af urgency for kunden kontra påvirkning af oppetid. Kunden skal altid via SLA gøres opmærksom på gældende procedure for vurderingen.

For ændringer ikke i den primære serviceydelse, tager driftschefen stilling til, hvilken action der skal tages, og bærer alene ansvaret for, at det udføres korrekt og rettidigt. Implementering af ændringer følger fast procedure.

12.1.3 Kapacitetsstyring

VUCHosting overvåger systemerne og netværket, så vi kan være proaktive, hvis der er alarmer. I samspil med overvågningen kan brugere indmelde kapacitetsproblemer til hotline. Disse kan føre til, at projektleder indstiller til driften, at kapacitet øges for den enkelte skole.

12.1.4 Adskillelse af miljøer

Miljøerne (Sandkasse, PreTest og Drift) afvikles på forskellige netværk og i forskellige zoner.

12.2 Beskyttelse mod Malware

Brugerne har ingen rettigheder til at eksekvere filer, som VUCHosting ikke har publiceret.

12.3 Backup

12.3.1 Sikkerhedskopiering af informationer

Vi sikrer at kunne genskabe systemer og data på hensigtsmæssig og korrekt vis og efter de aftaler, vi har med vores kunder. Omfanget af backup er formelt beskrevet i SLA for backup.

Vi har etableret en testplan for verificering af, hvorvidt sikkerhedskopieringen fungerer samt en test af, hvordan systemer og data praktisk kan retableres. Der føres en log over disse tests, således at vi kan følge op på, om vi kan ændre på procedurer og processer for at højne vores løsning. Testplanen lægges i en tasklist og en kalender, som påminder VUCHostings medarbejdere om dette.

Hver nat føres en fuld kopi af data fra vores centrale systemer til skyen ved hjælp af vores backup-system. Dermed er data separeret fra vores driftssystemer efter endt afvikling. Hver dag modtages log fra backup-jobbet med advarsel om eventuelle fejl. Denne modtages af minimum 2 medarbejdere. Den driftsansvarlige bærer ansvaret for at tjekke loggen og sørge for at genoprette backup.

12.4 Logning og overvågning

12.4.1 Hændelseslogning

Vi har opsat overvågning og logning af netværkstrafik, og vores driftsafdeling følger dette. Vi foretager ikke proaktiv overvågning af logførte hændelser, men følger op såfremt vi mistænker, at en hændelse kan relatere til forhold afdækket i log.

Til styring af overvågning og opfølgning på hændelser har vi formelle incident management-procedurer til sikring af, at hændelser registreres og håndteres, og at der foretages de nødvendige afhjælpninger.

VUCHosting har implementeret hændelseslogning til registrering af brugeraktivitet.

12.4.4 Tidssynkronisering

VUCHosting synkroniserer de primære domænecontrollere til en NTP-service og lader alle øvrige servere i det pågældende domæne hente deres tid derfra.

12.5 Styring af software på driftssystemer

12.5.1 Installation af programmer på driftssystemer

Vi sikrer, at der alene installeres godkendte og testede opdateringer på systemerne – herunder sikkerhedsopdateringer fra Microsoft, VMware og Cisco.

Ændringer, der har betydning for VUC'ernes drift, godkendes af projektlederen og implementering følger efter analyse af urgency kontra nedetid. Først herefter foretages ændringen eller opdateringen.

Inden hver opdatering planlægges fallback og restore.

For at sikre rettidig opdatering laves der en opdateringsplan for minimum indeværende år. Denne offentliggøres på VUCHostings hjemmeside.

12.6 Sårbarhedsstyring

12.6.1 Styring af tekniske sårbarheder

VUCHosting gør kun brug af hardware med gældende serviceaftaler. Kan en given serviceaftale ikke forlænges, indkøbes nyt hardware i stedet. Windows Server OS patches via WSUS.

Sikkerhedsudstyr skal patches løbende efter vurdering, dog minimum årligt. Ansvar for vurderingen alene ligger på den driftsansvarlige.

VUCHosting har implementeret sårbarhedsstyring, som løbende rapporterer risici. Rapporteringer om sårbarheder samt trusler indgår i den kommunikerede risikovurdering.

12.6.2 Begrænsning af programinstallering

Det er ikke muligt for eksterne brugere at installere programmer på VUCHostings servere. VUCHosting benytter provisioned images, som installeres centralt og benyttes til udrulning af et ubegrænset antal servere. Alle ændringer, som brugerne kan tilføje til serverne (indstillinger, midlertidige filer mv.), fjernes, når serveren genstartes.

Programinstallation kan kun ske i et særligt maintenance mode, som kun driftsmedarbejdere har adgang til at aktivere.

13 Kommunikationssikkerhed

13.1 Håndtering af netværkssikkerhed

13.1.1 Netværksforanstaltninger

Ansvaret for netværk og netværkssikkerhed er fastlagt, og der er udarbejdet procedurer, vejledninger og dokumentation til anvendelse i forbindelse med drift og vedligehold af netværket.

13.1.2 Sikring af netværkstjenester

VUCHosting er tjenesteudbyder af NemID. Brugerne tilgår ved hjælp af NemID, deres databaser som en 2-faktors godkendelse. Den driftsansvarlige har ansvaret for VUCHostings interne netværk og netværkssikkerhed fra VUCHostings lokation. Tilgang til og fra leverandør foregår via VPN-tunneller.

De enkelte VUC'er kan tilgå deres egne database hos VUCHosting via VPN. VUC'ernes VPN-adgang er dokumenteret hos VUCHosting.

Alene godkendt netværkstrafik (indgående) kommer gennem vores firewall. Der er etableres et DDoS-filter foran alt offentligt eksponeret netværksudstyr. Denne service, som er revideret efter ISAE 3402, stilles til rådighed af VUCHostings leverandør.

13.1.3 Opdeling af netværk

Netværket består af 3 zoner: Intern zone, sandkasse-zone og DMZ-zone. Adgang fra DMZ-zone til sandkasse-zone og intern zone er begrænset med firewall. Sandkasse-zonen er afskåret fra internetadgang.

13.2 Dataoverførsel

13.2.1 Politikker og procedurer for dataoverførsel

De enkelte VUC'er har en FTP-konto, som de kan tilgå nattens backup af deres database via. Databasen er krypteret. Eventuelt misbrug kan auditeres via log, som føres af VUCHosting.

Der er udarbejdet regelsæt for håndtering af data og dokumenter. Der er opsat faste regler for håndtering af de forskellige typer af dokumenter.

13.2.4 Fortrolighedsaftaler eller NDA (non-disclosure agreements)

Der er implementeret krav om indgåelse af NDA fra VUCHostings underleverandører, hvis VUCHosting vurderer dette nødvendigt.

14 Anskaffelse, udvikling og vedligeholdelse

14.2 Sikkerhed i udviklings- og støtteprocesser

14.2.2 Procedurer for styring af ændringer

Der er implementeret procedurer for styring af ændringer, således at disse styres og implementeres hensigtsmæssigt i forhold til VUC'ernes it-sikkerhed, nedetid og driftspåvirkning.

Alle ændringer idriftsættes på et fastsat tidspunkt. Det er aftalt med kunden, at der er et servicevindue til at lave rettelser og opgraderinger på systemet én gang om ugen. Der fortages fallback-planlægning, som sikrer, at ændringer kan rulles tilbage eller annulleres, hvis de ikke fungerer.

14.2.4 Begrænsning af ændringer af softwarepakker

EG udgiver nye releases minimum 12 gange årligt, og disse hentes ned fra hjemmeside stillet til rådighed af EG. VUCHosting modtager besked om nye releases både mundtligt og skriftligt og sikrer på den måde, at kun godkendte opdateringer lægges på.

14.2.5 Sikre systemudviklingsprincipper

Ludus suiten udvikles løbende i samarbejde med EG, som er leverandøren af softwaren. VUCHosting bærer ikke ansvaret for test af releases, men kan vælge at løfte opgaven i samarbejde med leverandøren, hvis en given opdatering er bestilt af VUCHostings projektleder. Hvis der har været bestilt udvikling, testes den af relevante slutbrugere fra sektoren. I oktober 2021 er efter forudgående forsøg indført fast pre-release-test samt regressionstest efter fast procedure, da leverandørens egen test ikke har vist sig af høj nok kvalitet.

Fundne fejl meldes ind til EG i en formel blanket og registreres i EG's incident management system.

14.2.6 Sikkert udviklingsmiljø

Testen foregår på særskilt testmiljø, og der testet udelukkende på egen institutions data. Adgang til testmiljøet styres via Citrix-adgang med NemID. Efter hver pre-release-test fjernes alle adgange til testmiljøet og nye relevante adgange tildeles først ved implementering af næste release.

15 Leverandørforhold

15.1 Informationssikkerhed i leverandørforhold

15.1.1 It-sikkerhedspolitik i forhold til leverandørforhold

VUCHosting skal indgå aftaler med alle leverandører i forhold til it-sikkerhed, for at imødegå de risici, der er forbundet med leverandørens adgange til vores aktiver. Gældende procedureskrivelser følges.

15.1.2 Sikkerhedsforhold i leverandøraftaler

Leverandører, som leverer systemer til VUCHosting, skal indgå formaliseret kontrakt såvel som databehandler- eller underdatabehandleraftaler med VUCHosting. VUCHosting anvender i nødvendigt omfang NDA-aftaler med leverandører, som ikke er kategoriseret som databehandlere.

15.2 Styring af serviceydelser fra tredjepart

15.2.1 Overvågning og evaluering af serviceydelser fra tredjeparter

Det kontrolleres årligt, om leverandørers ISAE 3402 er indhentet, og rapporten gennemgås. Kontrol for indhentning sker på driftsmøde i den daglige ledelse. Hvis den efterfølgende gennemgang af rapporten viser anseelige afvigelser konstateret, følges sikkerhedspolitikkens forskrifter for evt. handling.

16 Styring af sikkerhedshændelser

16.1 Styring af informationssikkerhedsbrud og forbedringer

16.1.1 Ansvar og procedurer

Driftsmedarbejderne og den driftsansvarlige holder sig opdaterede vha. leverandørers supporthjemmesider, debatfora, mailinglister mv. for konstaterede svagheder i de systemer, vi benytter og tilbyder. Alle ansatte i VUCHosting er underlagt pligt til at indberette mistanke om datalæk til KVUC's DPO og den driftsansvarlige.

16.1.2 Rapportering af informationssikkerhedshændelser

Informationssikkerhedshændelser registres i vores incident management-system. Rapportering til myndigheder og dataejer følger implementeret procedure.

17 Informationssikkerhedsaspekter ved beredskabsstyring

17.1 Beredskab

17.1.2 Implementering af nødplaner og procedurer

VUCHosting har en opdateret beredskabsplan.

17.1.3 Prøvning, vedligeholdelse og revurdering af beredskabsplaner

Beredskabsplanen reviewes og testes årligt og godkendes herefter af KVUC's øverste leder.

18 Overensstemmelse

18.1 Overensstemmelse med love og kontraktmæssige krav

18.1.1 Identifikation af gældende lovgivning og kontraktmæssige krav

VUCHosting har implementeret procedure for afdækning af myndighedskrav. Der er en klar ansvarsfordeling i den daglige ledelse i forhold til hvilke områder af lovgivning, den enkelte har ansvaret for at afdække. Nye myndighedskrav fremlægges på driftsmøder i den daglige ledelse.

18.2 Gennemgang af informationssikkerhed

18.2.2 Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder

Den daglige ledelse og driftsmedarbejderne udarbejder VUCHostings sikkerhedspolitik i fællesskab. Hotline informeres årligt om sikkerhedspolitikkens indhold, efter denne er påført ledelsesgodkendelse.

Da sikkerhedspolitikken er et arbejdsredskab, vil den ligge til grund for de relevante handlinger, der fortages i VUCHosting. Det er dermed ledelsens opfattelse, at sikkerhedspolitikken bliver efterlevet.

18.2.3 Kontrol af teknisk overensstemmelse

Ledelsen drøfter risici, ændringer, myndighedskrav med videre på driftsmøder, minimum efter behov. Dog minimum 4 gange årligt. For at sikre overensstemmelse imellem it-sikkerhedspolitikker og udførelsen af driften er alle driftsmedarbejdere involveret i udformningen og review af de gældende politikker.

Ændringer i perioden

Opdatering af Citrix Storefront
Nye databehandleraftaler med EG samt VUC'er
Webtilgængelighed på portal.vuchosting.dk

Komplementerende kontroller

VUCHostings kunder er, medmindre andet er aftalt, ansvarlige for at:

- Administrere og evaluere adgang til VUCHostings loginportal ved at oprette og nedlægge erhvervs-NemID for deres medarbejdere.
- Opbevare og distribuere kodeord til brugere samt sikkerhedsindstillinger i det hostede software.
- Foretage skriftlig godkendelse af alle leverandører, som ønsker adgang til kundens data via VPN-forbindelse.
- Angive, hvem der er superbrugere, it-ansvarlig og systemansvarlig, samt hvem der må få adgang til kundens testsystem.

4 Serviceleverandørs kontrolmål, kontroller, test og resultatet heraf

4.1 Introduktion

Denne rapport er udformet med henblik på at informere VUCHostings kunder om VUCHostings systemer og kontroller, som kan påvirke behandlingen af forretningsrelaterede transaktioner og samtidig informere VUCHostings kunder om funktionaliteten af de kontroller, der blev efterprøvet. Afsnittet, når det kombineres med en forståelse og vurdering af kontrollerne i brugerorganisationernes forretningsprocesser, har til hensigt at hjælpe brugerorganisationens revisor til at (1) planlægge revisionen af brugerorganisationens årsregnskaber og (2) vurdere risici for fejl i årsregnskaber, som muligvis påvirkes af de generelle it-kontroller hos VUCHosting.

Vores test af VUCHostings kontroller er begrænset til de kontrolmål og tilknyttede kontroller, som er nævnt i nedenstående kontrolmatrix i denne del af rapporten, og er ikke udvidet til at omfatte alle de kontroller, som er beskrevet i systembeskrivelsen, eller til de generelle it-kontroller, som skal være implementeret i brugerorganisationerne for at opfylde kontrolmålene. Det er hver brugerorganisations revisors ansvar at evaluere denne information i forhold til de kontroller, som eksisterer i hver brugerorganisation. Hvis bestemte supplerende kontroller ikke er til stede i brugerorganisationerne, kan VUCHostings kontroller muligvis ikke kompensere for sådanne svagheder.

4.2 Test af kontroller

De test, der udføres i forbindelse med fastlæggelsen af kontrollers funktionalitet, består af en eller flere af følgende metoder:

Metode	Beskrivelse
Forespørgsel	Forespørgsel hos udvalgt personale hos VUCHosting
Observation	Observation af kontrollens udførelse
Inspektion	Inspektion af dokumenter og rapporter, som indeholder angivelse af udførelsen af kontroller. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er udformet, så de kan forventes at blive effektive, hvis de implementeres. Endvidere vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Genudførelse af kontrollen	Gentagelse af den relevante kontrol med henblik på at verificere, at kontrollen fungerer som forudsat

4.3 Test af kontrollernes funktionalitet

Vores test af kontrollernes funktionalitet inkluderer de test, som vi betragter som nødvendige for at vurdere, om de udførte kontroller og overholdelsen heraf er tilstrækkelige til at give høj, men ikke absolut sikkerhed for, at de specificerede kontrolmål blev opnået i løbet af perioden fra 1. januar 2021 til 31. december 2021.

Vores test af kontrollernes funktionalitet var udformet til at dække et repræsentativt antal af transaktioner i løbet af perioden fra 1. januar 2021 til 31. december 2021 for hver kontrol, jf. nedenfor, som er udformet til at opnå de specifikke kontrolmål. Ved udvælgelsen af specifikke test har vi overvejet (a) karakteren af de testede områder, (b) typerne af tilgængelig dokumentation, (c) karakteren af de revisionsmål, der skal opnås, (d) det vurderede kontrolrisikoniveau og (e) testens forventede effektivitet.

4.4 Kontrolmål, kontroller og resultater af test

Kontrolmål, kontroller og resultater af test (ISO)
I nedenstående skema er de testede kontrolmål og kontroller anført, ligesom vi har beskrevet, hvilke revisionshandlinger, der er udført og resultatet af disse handlinger. I det omfang vi har konstateret væsentlige kontrolsvagheder, har vi anført dette.

Nr.	Kontrolmål og kontroller	Udførte test	Resultater af test
4 Risikovurdering og-håndtering			
4.1 Risikovurdering			
Formål: at sikre, at virksomheden periodisk foretager analyse og vurdering af it-risikobilledet.			
4.1.1	**It-risikoanalyse og -vurdering** Der er udarbejdet en ledelsesgodkendt risikovurdering, der opdateres minimum en gang om året.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings procedurer for risikoanalyse og -vurdering. Vi har inspiceret VUCHostings risikoanalyse og -vurdering og observeret, at den er opdateret og godkendt af ledelsen.	Ingen afvigelser konstateret.

Nr.	Kontrolmål og kontroller	Udførte test	Resultater af test
5 Sikkerhedspolitik			
5.1 It-sikkerhedspolitik			
Formål: at give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.			
5.1.1	**It-sikkerhedspolitik** Ledelsen fastlægger og godkender politikker for informationssikkerhed, som offentliggøres og kommunikeres til medarbejdere.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik samt observeret, at sikkerhedspolitikken er opdateret og godkendt af ledelsen. Vi har inspiceret dokumentation for, at sikkerhedspolitikken er gennemgået med VUCHostings medarbejdere på årligt møde.	Ingen afvigelser konstateret.
5.1.2	**Evaluering af it-sikkerhedspolitikken** Sikkerhedspolitikken evalueres årligt eller i tilfælde af væsentlige ændringer for at sikre dens fortsatte egnethed og tilstrækkelighed.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik samt observeret, at sikkerhedspolitikken er opdateret og godkendt af ledelsen.	Ingen afvigelser konstateret.

Nr.	Kontrolmål og kontroller	Udførte test	Resultater af test
6 Organisereting af informationssikkerhed			
6.1 Intern organisering			
Formål: at etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen.			
6.1.1	**Delegering af ansvar for informationssikkerhed** Alle ansvarsområder og rollefordelinger er klart defineret.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder procedure for delegering af ansvar for informationssikkerhed. Vi har inspiceret VUCHostings rollebeskrivelser og organisationsdiagram og observeret, at rollefordeling og ansvarsområder er klart defineret. Vi har observeret, at dokumenterne er opdateret og godkendt af ledelsen.	Ingen afvigelser konstateret.
6.1.2	**Funktionsadskillelse** For at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af organisationens aktiver er der indført funktionsadskillelse via rettighedsstyring.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder procedure for funktionsadskillelse. Vi har inspiceret udtræk fra Windows AD og observeret, at funktionsadskillelse sikres via tildeling af sikkerhedsroller.	Ingen afvigelser konstateret.
6.1.3	**Informationssikkerhed som en del af projektstyring** Der er etableret procedure for it-sikkerhed i projektstyring, og denne anvendes ved projektstyring, uanset projekttype.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder procedure for it-sikkerhed i projektstyring.	Vi har fået oplyst, at VUCHosting ikke har initieret nye projekter i erklæringsperioden. Det har derfor ikke været muligt at teste, hvorvidt proceduren for it-sikkerhed i projektstyring har været implementeret eller fungeret effektivt. Ingen afvigelser konstateret.

Nr.	Kontrolmål og kontroller	Udførte test	Resultater af test
6.2 Mobilt udstyr og fjernarbejdspladser			
Formål: at sikre fjernarbejdspladser og brugen af mobilt udstyr.			
6.2.1	**Politik for mobile enheder** VUCHosting har implementeret en politik for brug af mobile enheder, der har til formål at sikre, at adgang til Ludus sker på en betryggende måde.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder politik for mobile enheder. Vi har observeret, at adgang til Ludus fra mobile enheder alene kan ske via Ludus Web, som politikken foreskriver.	Ingen afvigelser konstateret.
6.2.2	**Fjernarbejdspladser** VUCHosting sikrer, at fjernadgang til systemerne sker via sikre og brugervenlige kanaler.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder relevante driftsprocedure. Vi har inspiceret dokumentation for setup af brugeradgang via Citrix-miljøet. Vi har inspiceret udtræk fra Windows AD, herunder brugeradgange der kan tilgå hostingmiljøet via VPN.	Vi har konstateret, at det er tilladt og muligt for VUCHostings it-driftsmedarbejdere at tilgå VUCHostings netværk og systemer via VPN-klient på it-udstyr uden for domænet, der ikke er underlagt krav til antivirus og malware-beskyttelse. Ingen yderligere afvigelser konstateret.

Nr.	Kontrolmål og kontroller	Udførte test	Resultater af test
7 Sikkerhed i forhold til ansættelse			
7.1 Inden ansættelse			
Formål: at sikre, at medarbejdere og kontrahenter forstår deres ansvar og er egnede til de roller, de er i betragtning til.			
7.1.1	**Screening** VUCHosting sørger for, at screening af nye medarbejdere som hovedregel sker via rekrutteringsbureauer. Hvis en af kandidaterne er kendt, foretages screening af ledelsen. Ved ansættelsessamtaler skal der være repræsentant fra ledelse samt fra medarbejdergruppen.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder procedure for ansættelse af medarbejdere.	Vi har konstateret, at VUCHosting ikke har ansat nye medarbejdere i erklæringsperioden. Det har derfor ikke været muligt at teste, hvorvidt proceduren vedrørende screening har været implementeret samt har fungeret effektivt. Ingen afvigelser konstateret.
7.1.2	**Ansættelsesforhold** I et tillæg til den ansattes kontrakt med KVUC anføres særlige forhold vedrørende fortrolighed i forbindelse med adgang til personfølsomme oplysninger for VUCHostings kunder.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret skabelon for ansættelsesbrev, som modtages i forbindelse med en ny ansættelse. Vi har inspiceret skabelon for erklæring om tavshedspligt og overholdelse af sikkerhedsregler, som underskrives i forbindelse med en ny ansættelse.	Vi har konstateret, at VUCHosting ikke har ansat nye medarbejdere i erklæringsperioden. Det har derfor ikke været muligt at teste, hvorvidt proceduren vedrørende fortrolighed i forbindelse med ansættelse har været implementeret samt har fungeret effektivt. Ingen afvigelser konstateret.
7.2 Under ansættelse			
Formål: at sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.			
7.2.1	**Ledelsens ansvar** Ledelsen kræver, at alle medarbejdere opretholder informationssikkerhed i overensstemmelse med organisationens fastlagte politikker og procedurer.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik og observeret, at denne er gennemgået sammen med relevante medarbejdere, hvorefter den er godkendt af ledelsen. Vi har inspiceret dokumentation for, at der aktivt gøres tiltag for, at medarbejderne er bekendte med politikker og procedurer, således, at informationssikkerheden opretholdes.	Ingen afvigelser konstateret.

Nr.	Kontrolmål og kontroller	Udførte test	Resultater af test
7.2.2	**Bevidsthed om uddannelse og træning i informationssikkerhed** VUCHosting anvender eksterne kurser og konferencer for at sikre, at medarbejdere opnår kompetencer, der kan matche virksomhedens behov og sikre fortsat niveau af it-sikkerhed. VUCHosting gennemfører årlige medarbejderudviklingssamtaler. Hvor det er relevant for den ansattes jobfunktion, sørger ledelsen for, at vedkommende er bekendt med opdaterede politikker og procedurer omkring it-sikkerhed.	Vi har udført forespørgsel hos passende personale. Vi har stikprøvevis inspiceret dokumentation for, at der bliver anvendt eksterne kurser og konferencer til fortsat at sikre det rette it-sikkerhedsniveau for VUCHosting. Vi har stikprøvevis inspiceret dokumentation for afholdte medarbejderudviklingssamtaler.	Ingen afvigelser konstateret.
7.3 Ansættelsesforholdets ophør eller ændring			
Formål: at beskytte organisationens interesser som led i ansættelsesforholdets ændring eller ophør.			
7.3.1	**Ophør eller ændring i ansættelse** Informationssikkerhedsansvar og tavshedspligt, som gælder efter ansættelsens ophør eller ændring, skal defineres og kommunikeres til medarbejderen.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder procedure vedrørende ophør eller ændring i ansættelse. Vi har inspiceret skabelon for erklæring om tavshedspligt og overholdelse af sikkerhedsregler.	Vi har konstateret, at VUCHosting ikke har haft nogen fratrædelser eller ændring i strukturen af medarbejdere i erklæringsperioden. Det har derfor ikke været muligt at teste, hvorvidt proceduren vedrørende informationssikkerhedsansvar og tavshedspligt har været implementeret samt har fungeret effektivt. Ingen afvigelser konstateret.

Nr.	Kontrolmål og kontroller	Udførte test	Resultater af test
8 Styring af aktiver			
8.1 Ansvar for aktiver			
Formål: at identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf.			
8.1.1	**Fortegnelse over aktiver** Aktiver i relation til information og informationsbehandlingsfaciliteter skal identificeres, og der skal udarbejdes og vedligeholdes en fortegnelse over disse aktiver.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret proceduren for styring af aktiver. Vi har observeret, at der er føres en fortegnelse, hvori aktiver beskrives. Vi har inspiceret dokumentation for, at der i denne fortegnelse forekommer oversigt over, hvilke aktiver VUCHosting har ansvaret for samt, at fortegnelsen er gennemgået af driftsansvarlige i erklæringsperioden.	Ingen afvigelser konstateret.
8.1.2	**Ejerskab af aktiver** Der skal være udpeget en driftsansvarlig, og denne skal være bevist om rolle som ejer af aktiver.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret dokumentation for VUCHostings rollebeskrivelser og organisationsdiagram og observeret, at ansvaret for drift og ejerskab af aktiver er klart defineret. Vi forespurgt, om den driftsansvarlige er bevidst om sit ansvar som ejer af aktiver, hvoraf han har bekræftet.	Ingen afvigelser konstateret.
8.1.3	**Klassifikation af information** VUCHosting skal have politik for klassifikation af data.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik. Vi har inspiceret politik for klassifikation af data.	Vi har konstateret, at der er implementeret en procedure for klassifikation af data, som sikrer passende klassificering af data. Vi har dog konstateret, at politikken ikke omfatter krav til opbevaring og beskyttelse af data. Ingen yderligere afvigelser konstateret.
8.1.4	**Tilbagelevering af aktiver** Alle ansatte kvitterer for tilbageaflevering af udleverede computere og mobile enheder, ved endt brug.	Vi har udført forespørgsel hos passende personale.	Vi har konstateret, at der ikke er blevet tilbageleveret aktiver i forbindelse med endt brug i er-

Nr.	Kontrolmål og kontroller	Udførte test	Resultater af test
		Vi har inspiceret procedure vedrørende vilkår ved lån af udstyr.	klæringsperioden. Vi har derfor ikke kunnet teste, at ansatte kvitterer for tilbagelevering af udleveret udstyr ved endt brug. Ingen afvigelser konstateret.
8.3 Mediehåndtering			
Formål: at forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier.			
8.3.2	**Bortskaffelse af medier** Medier bortskaffes på forsvarlig vis, når de er defekte, eller der ikke længere er brug for dem.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik og observeret, at denne indeholder afsnit omkring håndtering af bærbare medier.	Vi har konstateret, at der ikke har været bortskaffelse og destruktion af medier i erklæringsperioden. Vi har derfor ikke kunnet teste, at medier bortskaffes på forsvarlig vis. Ingen afvigelser konstateret.

Nr.	Kontrolmål og kontroller	Udførte test	Resultater af test
9 Adgangskontrol			
9.1 Forretningskrav til adgangskontrol			
Formål: at begrænse adgangen til information og informationsbehandlingsfaciliteter.			
9.1.1	**Politikker for adgangsstyring** VUCHosting har defineret politikker for adgangsstyring, der er beskrevet i den til enhver tid gældende sikkerhedspolitik.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder procedure og retningslinjer for adgangskontrol for interne såvel som eksterne medarbejdere. Vi har observeret, at sikkerhedspolitikken er godkendt af ledelsen.	Ingen afvigelser konstateret.
9.2 Administration af brugeradgang			
Formål: at sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.			
9.2.1	**Brugeroprettelses- og nedlæggelsesprocedure** VUCHosting har implementeret formelle procedure for tildeling af brugeradgange samt tilbagekaldelse af rettigheder. Der er implementeret procedure, som sikrer, at adgangsrettigheder inddrages, hvor der ikke længerede eksisterer et arbejdsbetinget behov.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder procedure og retningslinjer for adgangskontrol for interne såvel som eksterne medarbejdere.	Vi har konstateret, at der ikke er fratrådt eller ansat nye medarbejdere i erklæringsperioden. Det har derfor ikke været muligt at teste, hvorvidt proceduren vedrørende adgangsfratagelse eller tildeling af adgange har været implementeret samt har fungeret effektivt. Ingen afvigelser konstateret.
9.2.2	**Rettighedstildeling** Ledelsen har ansvaret for den interne tildeling af administratorrettigheder samt rettigheder for almindelige interne brugere. Den driftsansvarlige godkender desuden tildeling og varighed af administratorrettigheder til leverandører via underskrevne aftaler med leverandøren.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder procedure og retningslinjer for adgangskontrol for interne såvel som eksterne medarbejdere. Vi har inspiceret udtræk af bruger og sikkerhedsroller fra Windows AD og observeret, at rettigheder er tildelt ud fra et arbejdsbetinget behov. Vi har stikprøvevis inspiceret, at driftsansvarlig har godkendt tildeling og varighed af	Ingen afvigelser konstateret.

Nr.	Kontrolmål og kontroller	Udførte test	Resultater af test
		administratorrettigheder til ekstern konsulent via underskrevne aftaler med konsulenten.	
9.2.3	**Kontrol med privilegerede adgangsrettigheder** VUCHosting sørger for at den driftsansvarlige dagligt tilsendes en aktivitetsrapport over brugeraktivitet for privilegerede brugere.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder procedure for styring og overvågning af privilegerede adgangsrettigheder. Vi har stikprøvevis inspiceret aktivitetsrapporter på logning af administratoradgange og brugeraktivitet.	Ingen afvigelser konstateret.
9.2.4	**Håndtering af fortrolige logininformationer** Alle ansatte i VUCHosting bliver via informationsbrev, der medfølger NemID-nøglekort, informeret om håndtering af fortrolige logininformationer.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder procedure for brugeransvar.	Vi har konstateret, at VUCHosting ikke har ansat nye medarbejdere i erklæringsperioden. Det har derfor ikke været muligt at teste, hvorvidt nye medarbejdere modtager informationsbrev. Ingen afvigelser konstateret.
9.2.5	**Evaluering af brugeradgangsrettigheder** Alle brugerrettigheder for ansatte i VUCHosting evalueres løbende af ledelsen.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret proceduren for gennemgang af brugernes adgangsrettigheder. Vi har inspiceret dokumentation for den årlige gennemgang af alle brugeres adgangsrettigheder. Vi har stikprøvevis inspiceret aktivitetsrapporter på logning af administratoradgange og brugeraktivitet.	Ingen afvigelser konstateret.
9.4 Kontrol af adgang til systemer og data			
Formål: at forhindre uautoriseret adgang til systemer og applikationer.			
9.4.1	**Begrænset adgang til data** Adgang til systemer er baseret på arbejdsbetinget behov, og proces for adgangsstyring er beskrevet i VUC Hostings informationssikkerhedspolitik.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder procedure for adgangsstyring.	Ingen afvigelser konstateret.

Nr.	Kontrolmål og kontroller	Udførte test	Resultater af test
		Vi har inspiceret udtræk over brugere og sikkerhedsroller i Windows AD og observeret, at VUC-skolernes adgange til Citrix-miljøet er styret via sikkerhedsroller i Windows AD. Vi har observeret, at adgange til fortrolig information på fileshare er styret via NTFS-rettigheder. Vi har stikprøvevis inspiceret adgangstildeling til FTP-serveren.	
9.4.2	**Procedure for sikker log-on** Hvis det kræves i henhold til politikken for adgangsstyring, skal adgang til systemer og applikationer styres af en procedure for sikker log-on.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder procedure for sikker log-on samt procedure for NemID og sikkerhed. Vi har inspiceret udtræk over brugere og sikkerhedsroller fra Windows AD. Vi har observeret, at password opbevares på fortroligt drev, hvor adgange hertil styres via NFTS-rettigheder.	Ingen afvigelser konstateret.
9.4.3	**System for administration af adgangskoder** VUCHosting har implementeret systemer til administration af adgangskoder, der sikrer adgangskoder med god kvalitet og hyppig udskiftning.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder procedure for anvendelse af passwords. Vi har inspiceret passwordkonfigurationen via opsat Default domain policy og verificeret, at denne som minimum matcher VUCHostings krav.	Ingen afvigelser konstateret.

Nr.	Kontrolmål og kontroller	Udførte test	Resultater af test
10 Kryptografi			
10.1 Kontrol med anvendelsen af kryptografi			
Formål: at sikre korrekt og effektiv brug af kryptografi for at beskytte informationers fortrolighed, autenticitet og/eller integritet.			
10.1.1	**Politik for anvendelse af kryptografi** VUCHosting har udarbejdet og implementeret en politik for anvendelse af kryptografi til beskyttelse af information.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder procedure for regler for anvendelse af kryptografi. Vi har inspiceret AlphaSSL-krypteringscertifikater og observeret, at adgang til Ludus Web og Citrix-miljø er krypteret med anerkendt krypteringsalgoritme. Vi har observeret, at krypteringscertifikaterne er gyldige i hele erklæringsperioden.	Ingen afvigelser konstateret.
10.1.2	**Administration af krypteringsnøgler** VUCHosting har implementeret en politik for anvendelse og opbevaring af krypteringsnøgler.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder retningslinjer for anvendelse af kryptografi. Vi har inspiceret skabelon for VPN-blanket til oprettelse af krypteret VPN-forbindelse mellem VUCHostings miljø og VUC-skolerne. Vi har observeret, at krypteringsnøgler opbevares på fortroligt drev.	Ingen afvigelser konstateret.

Nr.	Kontrolmål og kontroller	Udførte test	Resultater af test
11 Fysisk og miljømæssig sikring			
11.1 Sikre områder			
Formål: at forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.			
11.1.2	**Fysisk adgangskontrol** VUCHosting sikrer, at kun autoriserede medarbejdere har adgang til datacentret.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder procedure for kontrol af fysisk adgangskontrol. Vi har inspiceret adgangsliste for personer hos VUCHosting, der har adgang til datacentret hos GlobalConnect.	Ingen afvigelser konstateret.
11.1.3	**Sikring af kontorer, lokaler og faciliteter** Der er implementeret fysisk sikring af kontorer, lokaler og faciliteter i VUCHosting.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret procedure for sikring af VUCHostings kontorer, lokaler og faciliteter. Vi har ved besøg hos VUCHosting observeret, at der er etableret lås på døren med adgangskort og videoovervågning af driftskonteret. Vi har stikprøvevis inspiceret dokumentation for, at al adgang til kontorerne logges.	Ingen afvigelser konstateret.
11.2 Udstyr			
Formål: at undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen.			
11.2.7	**Sikker bortskaffelse eller genbrug af udstyr** Alt databærende udstyr bortskaffes, ved endt brug.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret procedure for bortskaffelse af databærende udstyr.	Der ikke har været foretaget destruktion af medier i erklæringsperioden, hvorfor det ikke har været muligt at teste, om proceduren for bortskaffelse er implementeret og har fungeret effektivt i erklæringsperioden. Ingen afvigelser konstateret.

Nr.	Kontrolmål og kontroller	Udførte test	Resultater af test
11.2.8	**Brugerudstyr uden opsyn** VUCHosting har implementeret politik om passwordbeskyttet pauseskærm til at sikre, at udstyr, som er uden opsyn, er passende beskyttet.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder proceduren for automatisk lås af skærm. Vi har observeret, at den etablerede sikkerhedsopsætning på VUCHosting AD-domæne sikrer, at arbejdsstationer låses efter en periode uden aktivitet.	Ingen afvigelser konstateret.
11.2.9	**Politik for ryddeligt skrivebord og blank skærm** VUCHosting har implementeret en politik om at holde skriveborde ryddet for papir og flytbare lagringsmedier og om blank skærm på informationsbehandlingsfaciliteter.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret dokumentation for, at der er etableret en "clean desk policy", som foreskriver, at fortrolige dokumenter skal være låst væk, når disse ikke anvendes. Vi har stikprøvevist inspiceret kontorer hos VUCHosting og observeret, at ubemandede skriveborde var ryddet.	Ingen afvigelser konstateret.

Nr.	Kontrolmål og kontroller	Udførte test	Resultater af test
12 Sikkerhed i forbindelse med drift			
12.1 Operationelle procedure og ansvarsområder			
Formål: at sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.			
12.1.1	**Dokumenterede driftsprocedurer** VUCHosting har dokumenterede driftsprocedurer, som er tilgængelige for alle brugere, der har brug for dem.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret driftsprocedure, og at disse er opbevaret på og tilgængelig for VUCHostings medarbejdere.	Ingen afvigelser konstateret.
12.1.2	**Ændringsstyring** VUCHosting har implementeret procedurer, som sikrer, at ændringer håndteres gennem test og godkendelser.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder procedure for ændringsstyring. Vi har inspiceret procedurer for håndtering af planlagte patches og sikkerhedsadviseringer, der omfatter Windows Server 2012 R2. Vi har stikprøvevist inspiceret dokumentation for, at der er foretaget månedlig patching af servere og netværksenheder som planlagt.	Ingen afvigelser konstateret.
12.1.3	**Kapacitetsstyrring** VUCHosting har etableret overvågning af ressourcer og kapacitet via overvågningssystemer.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder procedure for kapacitetsstyrring, som er beskrevet gennem driftsprocedurerne. Vi har observeret, at der anvendes overvågningssystem i forbindelse med overvågning af ressourcer og kapacitet.	Ingen afvigelser konstateret.
12.1.4	**Adskillelse af miljøer** Udviklings-, test- og driftsmiljøer er adskilte for at nedsætte risikoen for uautoriseret adgang til eller ændringer af driftsmiljøet.	Vi har udført forespørgsel hos passende personale.	Ingen afvigelser konstateret.

Nr.	Kontrolmål og kontroller	Udførte test	Resultater af test
		Vi har inspiceret VUCHostings sikkerhedspolitik, herunder procedure for teknisk infrastruktur, hvor der redegøres for anvendte miljøer. Vi har inspiceret VUCHostings netværkstopologi samt observeret, at forskellige miljøer er etableret, samt at de er logisk adskilte.	
12.2 Beskyttelse mod malware			
Formål: at sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.			
12.2.1	**Beskyttelse mod malware** Det er sikret, at brugere ikke har rettigheder til at eksekvere filer, som VUCHosting ikke har publiceret.	Vi har udført forespørgsel hos passende personale. Vi har observeret, at der ikke kan eksekveres EXE-filer på Citrix-miljøet. Vi har stikprøvevis inspiceret dokumentation for, at der er installeret antivirus på VUCHostings medarbejderes arbejdsstationer, samt at antivirussen er opdateret.	Ingen afvigelser konstateret.
12.3 Backup			
Formål: at beskytte mod tab af data.			
12.3.1	**Sikkerhedskopiering af informationer** Der tages backupkopier af databaser, centrale systemer og filer og disse testes regelmæssigt i overensstemmelse med backuppolitikken.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder driftsprocedure for backup. Vi har stikprøvevis inspiceret dokumentation på notifikationse-mails på daglig backup. Vi har stikprøvevis inspiceret dokumentation for udført restore-test af backup af databaser for erklæringsperioden.	Ingen afvigelser konstateret.
12.4 Logning og overvågning			
Formål: at registrere hændelser og tilvejebringe bevis			
12.4.1	**Hændelseslogning**	Vi har udført forespørgsel hos passende personale.	

Nr.	Kontrolmål og kontroller	Udførte test	Resultater af test
	VUCHosting har implementeret hændelseslogning til registrering af brugeraktivitet og overvågning af netværkstrafik. VUCHosting har implementeret procedurer til sikring af, at hændelser registreres og håndteres.	Vi har inspiceret VUCHostings sikkerhedspolitik. Vi har stikprøvevis inspiceret aktivitetsrapporter på logning af administratoradgange og brugeraktivitet.	Vi har konstateret, at der ikke foreligger en formel og ledelsesgodkendt procedure for overvågning af netværkstrafik til sikring af, at hændelser registreres og håndteres. Ingen yderligere afvigelser konstateret.
12.4.2	**Tidssynkronisering** VUCHosting synkronisere alle relevante systemer til en enkelt referencetidsangivelseskilde.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings NTP-konfiguration.	Ingen afvigelser konstateret.
12.5 Styring af driftssoftware på driftssystemer			
Formål: at sikre integriteten af driftssystemer.			
12.5.1	**Installation af programmer på driftssystemer** VUCHosting har implementeret procedurer til styring af softwareinstallationen på driftssystemer.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik. Vi har stikprøvevis inspiceret dokumentation for patchning af sikkerhedsopdatering på Windows-servere.	Vi har konstateret, at der ikke foreligger en formel og ledelsesgodkendt procedure til at sikre korrekt styring af softwareinstallationer i driftssystemer. Ingen yderligere afvigelser konstateret.
12.6 Sårbarhedsstyring			
Formål: at forhindre, at tekniske sårbarheder udnyttes.			
12.6.1	**Styring af tekniske sårbarheder** VUCHosting har implementeret sårbarhedsstyring, som løbende rapporterer risici. Rapporteringer om sårbarheder samt trusler indgår i den kommunikerede risikovurdering.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik. Vi har stikprøvevis inspiceret rapporteringer, som den driftsansvarlige har modtaget i forbindelse med sårbarheder. Vi har inspiceret VUCHostings risikovurdering og observeret, at den er opdateret og godkendt af ledelsen.	Vi har konstateret, at der ikke foreligger en formel procedure for styring af tekniske sårbarheder, som sikrer, at sårbarheder i anvendte informationssystemer evalueres, og at der iværksættes passende foranstaltninger for at håndtere den tilhørende risiko. Ingen yderligere afvigelser konstateret.

Nr.	Kontrolmål og kontroller	Udførte test	Resultater af test
12.6.2	**Begrænsning af programinstallering** VUCHosting har implementeret regler om softwareinstallation, som foretages af brugerne.	Vi har udført forespørgsel hos passende personale. Vi har observeret, at der ikke kan eksekveres EXE-filer på Citrix-miljøet.	Ingen afvigelser konstateret.

Nr.	Kontrolmål og kontroller	Udførte test	Resultater af test
13 Kommunikationssikkerhed			
13.1 Håndtering af netværkssikkerhed			
Formål: at sikre beskyttelse af informationer i netværk og understøttende informationsbehandlingsfaciliteter.			
13.1.1	**Netværksforanstaltninger** VUCHostings netværk styres og kontrolleres for at beskytte informationer i systemer og applikationer.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret dokumentation for det overordnede netværk og vurderet omfanget og kvaliteten af den udarbejdede dokumentation. Vi har inspiceret dokumentation for etablering af firewall på klienter og servere.	Ingen afvigelser konstateret.
13.1.2	**Sikring af netværkstjenester** VUCHosting har implementeret sikkerhedsmekanismer og styringskrav til alle netværkstjenester.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret dokumentation for det overordnede netværk og har vurderet omfang og kvalitet af den udarbejdede dokumentation. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder procedure for VPN-adgang og NEM ID-løsningen. Vi har inspiceret skabelon for forespørgsler på tildeling af VPN-adgang for skolerne. Vi har inspiceret dokumentation for 2-faktor autentificering ved login via NemID.	Ingen afvigelser konstateret.
13.1.3	**Opdeling af netværk** VUCHostings netværk er opdelt i relevante zoner.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings netværkstopologi samt observeret, at der er implementeret segmentering af netværket med firewalls samt separate VLAN i forskellige DMZ-zoner.	Ingen afvigelser konstateret.

Nr.	Kontrolmål og kontroller	Udførte test	Resultater af test
13.2 Dataoverførsel			
Formål: at opretholde informationssikkerhed ved overførsel internt i en organisation og til en ekstern entitet.			
13.2.1	**Politikker og procedurer for dataoverførsel** VUCHosting har implementeret formelle politikker, procedurer og overvågning for overførsel af data.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret procedure for dataoverførelse FTP samt procedure for deling af kodeord. Vi har observeret, at kryptering anvendes, og at der fra de enkelte VUC-skoler anvendes en FTP-server til dataoverførsel. Vi har inspiceret dokumentation for, at fjernadgange foretages via en godkendt, sikker kommunikationsforbindelse og klient.	Ingen afvigelser konstateret.
13.2.4	**Fortrolighedsaftaler eller NDA (non-disclosure agreements)** VUCHosting har implementeret krav om indgåelse af NDA fra VUCHostings underleverandører, hvis VUCHosting vurderer dette nødvendigt.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret procedure for valg af it-leverandør.	Vi har konstateret, at der ikke har været nogen tilfælde af indgåede NDA for erklæringsperioden. Ingen afvigelser konstateret.

Nr.	Kontrolmål og kontroller	Udførte test	Resultater af test
14 Anskaffelse, udvikling og vedligeholdelse			
14.2 Sikkerhed i udviklings- og støtteprocesser			
Formål: at sikre, at informationssikkerhed tilrettelægges og implementeres inden for informationssystemers udviklingscyklus.			
14.2.2	**Procedurer for styring af ændringer** Ændringer af Ludus Suite, som er bestilt af VUCHosting, styres ved hjælp af formelle procedurer for ændringsstyring.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder proceduren for ændringsstyring ved ændringer af Ludus Suite.	Vi har konstateret, at VUCHosting ikke har bestilt ændringer i erklæringsperioden. Vi har derfor ikke kunnet teste, at procedure og kontrol for sikre systemudviklingsprincipper er implementeret samt har fungeret effektivt. Ingen yderligere afvigelser konstateret.
14.2.4	**Begrænsning af ændringer af softwarepakker** Ændringer i Ludus Suite er begrænset til nødvendige ændringer, og alle ændringer styres effektivt.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder proceduren for ændringsstyring ved ændringer af Ludus Suite. Vi har stikprøvevis inspiceret releases og systemopdateringer i erklæringsperioden og observeret, at alle opdateringer er dokumenteret med versionsbrev, hvorved det sikres, at ændringer til Ludus web og Ludus + DB er dokumenteret. Vi har stikprøvevist observeret, at der fremsendes release e-mail fra serviceunderleverandøren EG A/S, når ny release forligger.	Ingen afvigelser konstateret.
14.2.5	**Sikre systemudviklingsprincipper** VUCHosting har implementeret fastlagte principper for udvikling og test af Ludus Suite, som skal dokumenteres, opretholdes og anvendes i forbindelse med alle bestilte ændringer.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder proceduren for ændringsstyring ved ændringer af Ludus Suite.	Vi har konstateret, at VUCHosting ikke har bestilt ændringer i erklæringsperioden. Vi har derfor ikke kunnet teste, at procedure og kontrol for sikre systemudviklingsprincipper er implementeret samt har fungeret effektivt. Ingen yderligere afvigelser konstateret.

Nr.	Kontrolmål og kontroller	Udførte test	Resultater af test
14.2.6	**Sikkert udviklingsmiljø** VUCHosting har etableret et sikkert og særskilt udviklings- og testmiljø. Udvikling og vedligeholdelse af Ludus er outsourcet til EG A/S, herunder etablering af udviklingsmiljøet.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings netværkstypologi og observeret, at test og produktionsmiljøer er adskilte. Vi har inspiceret procedure for navnestandard for servere og servicekonti samt observeret, at der er oprettet DMZ-zone for hver VUC-skole, hvor testmiljø er placeret.	Ingen afvigelser konstateret.

Nr.	Kontrolmål og kontroller	Udførte test	Resultater af test
15 Leverandørforhold			
15.1 – Informationssikkerhed i leverandørforhold			
Formål: at sikre beskyttelse af organisationens aktiver, som leverandører har adgang til			
15.1.1	**It-sikkerhedspolitik i forhold til leverandørforhold** VUCHosting har indgået aftaler med alle leverandører i forhold til it-sikkerhed for at imødegå de risici, der er forbundet med leverandørens adgange til aktiver. Aftalerne er dokumenteret.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings procedure for valg af it-leverandører. Vi har stikprøvevist inspiceret indgåede aftalekontrakter med relevante serviceunderleverandører.	Ingen afvigelser konstateret.
15.1.2	**Sikkerhedsforhold i leverandøraftaler** Leverandører, som leverer systemer til VUCHosting, indgår formaliseret kontrakt såvel som databehandler-, underdatabehandleraftaler eller NDA med VUCHosting.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings procedure for valg af it-leverandører. Vi har inspiceret underdatabehandleraftaler gældende for de ydelser, som EG A/S og Atea Managed Services leverer, herunder udvikling og vedligeholdelse af Ludus Suite samt ekstern backup.	Ingen afvigelser konstateret.
15.2 – Styring af serviceydelser fra tredjepart			
Formål: at opretholde et aftalt niveau af informationssikkerhed og levering af ydelser i henhold til leverandøraftalerne			
15.2.1	**Overvågning og evaluering af serviceydelser fra tredjeparter** VUCHosting overvåger og reviderer regelmæssigt leverandørydelser ved indhentning og gennemgang af ISAE 3402-erklæringer.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings procedure for evaluering af serviceunderleverandører. Vi har observeret, at VUCHosting indhenter relevante revionserklæringer fra it-leverandører samt gennemgår og vurderer eventuelle konstaterede afvigelser på driftsmøde.	Ingen afvigelser konstateret.

Nr.	Kontrolmål og kontroller	Udførte test	Resultater af test
16 Styring af sikkerhedshændelser			
16.1 – Styring af informationssikkerhedsbrud og forbedringer			
Formål: at sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder kommunikation om sikkerhedshændelser og –svagheder			
16.1.1	**Ansvar og procedurer** Ledelsesansvar, dataansvar og procedurer er fastlagt for at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings procedure for håndtering af sikkerhedsbrud og observeret, at den klart beskriver rolle og ansvarsfordeling i forbindelse med håndtering af sikkerhedshændelser.	Der er ikke konstateret informationssikkerhedsbrud i erklæringsperioden, vi har derfor ikke kunne teste, at proceduren for håndtering af sikkerhedsbrud er implementeret og har fungeret effektivt. Ingen afvigelser konstateret.
16.1.2	**Rapportering af informationssikkerhedshændelser** Informationssikkerhedshændelser rapporteres ad passende ledelseskanaler og registreres i incident management-system.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings procedure for håndtering af sikkerhedsbrud og observeret, at den klart beskriver rolle- og ansvarsfordeling i forbindelse med håndtering af sikkerhedshændelser.	Der er ikke konstateret informationssikkerhedsbrud i erklæringsperioden, vi har derfor ikke kunne teste, at proceduren for håndtering af sikkerhedsbrud er implementeret og har fungeret effektivt. Ingen afvigelser konstateret.

Nr.	Kontrolmål og kontroller	Udførte test	Resultater af test
17 informationssikkerhedsaspekter ved beredskabsstyring			
17.1 – Beredskab			
Formål: Beredskabsstyringen skal være forankret i VUCHostings ledelsessystemer.			
17.1.2	**Implementering af nødplaner og procedurer** VUCHosting har fastlagte, dokumenterede og opdaterede, procedurer og kontroller for at sikre hurtig og effektiv afhjælpning i kritiske situationer.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings beredskabsplan og observeret, at den definerer roller og ansvarsområder ved aktivering af beredskabet, samt hvornår beredskabet skal aktiveres. Vi har observeret, at beredskabsplanen er opdateret og godkendt af ledelsen.	Ingen afvigelser konstateret.
17.1.3	**Prøvning, vedligeholdelse og revurdering af beredskabsplaner** VUCHosting afprøver de fastlagte, dokumenterede, procedurer og kontroller med henblik på at sikre, at de er tidssvarende og effektive i kritiske situationer.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder procedure for informationssikkerhedsaspekter ved bredskabsstyring. Vi har inspiceret dokumentation for udført beredskabstest.	Ingen afvigelser konstateret.

Nr.	Kontrolmål og kontroller	Udførte test	Resultater af test
18 Overensstemmelse			
18.1 - Overensstemmelse med love og kontraktmæssige krav			
Formål: at forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav			
18.1.1	**Identifikation af gældende lovgivning og kontraktmæssige krav** VUCHosting har implementeret procedure for afdækning af myndighedskrav.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings procedure for afdækning af myndighedskrav. Vi har stikprøvevis inspiceret referater for afholdte driftsmøder i erklæringsperioden og observeret, at der her sker vidensdeling af nye myndighedskrav med betydning for VUCHosting.	Ingen afvigelser konstateret.
18.2 Gennemgang af informationssikkerhed			
Formål: at sikre, at informationssikkerhed er implementeret og drives i overensstemmelse med VUCHostings politikker og procedurer			
18.2.2	**Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder** De driftsansvarlige undersøger regelmæssigt, om procedurerne inden for deres ansvarsområde er i overensstemmelse med relevante sikkerhedspolitikker.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder udarbejdet driftsprocedure. Vi har inspiceret referat for afholdt driftsmøde i erklæringsperioden og observeret, at driftsprocedurer og sikkerhedspolitikken er gennemgået. Vi har inspiceret dokumentation for afholdt møde med it-driftsmedarbejdere, hvor sikkerhedspolitikken er blevet gennemgået.	Ingen afvigelser konstateret.
18.2.3	**Kontrol af teknisk overensstemmelse** Systemer undersøges regelmæssigt for overensstemmelse med VUCHostings informationssikkerhedspolitikker og -standarder.	Vi har udført forespørgsel hos passende personale. Vi har inspiceret VUCHostings sikkerhedspolitik, herunder udarbejdede driftsprocedurer. Vi har inspiceret referat for afholdt driftsmøde i erklæringsperioden og observeret, at	Ingen afvigelser konstateret.

Nr.	Kontrolmål og kontroller	Udførte test	Resultater af test
		driftsprocedurer og sikkerhedspolitikken er gennemgået. Vi har inspiceret dokumentation for afholdt møde med it-driftsmedarbejdere, hvor sikkerhedspolitikken er blevet gennemgået.	